CLAIMS:

1. A method of enabling authenticated communication of information between at least a primary entity and each of one or more secondary entities, each of the one or more secondary entities having an identifier associated with it, the method including the steps of:

allocating first secret information to the primary entity;

for each of the one or more secondary entities, determining second secret information, the second secret information being the result of a one way function applied to that second secret entity's identifier and the first secret information;

allocating the second secret information to the or each secondary entity.

2. A method according to claim 1, wherein the identifiers allocated to the secondary entities are generated stochastically, pseudo-randomly or arbitrarily.

3. A method according to claim 2, wherein the one way function is a hash function.

4. A method according to claim 3, wherein the first secret information is a key.

5. A method according to claim 3, wherein the one way function is a SHA function.

6. A method according to claim 1, wherein each of the entities is implemented in an integrated circuit.

7. A method according to claim 1, wherein each of the entities is implemented in an integrated circuit separate from the integrated circuits in which the other entities are implemented.

8. A method according to claim 1, wherein one or more of the secondary entities are implemented in a corresponding plurality of integrated circuits.

9. A method according to claim 1, wherein the primary entity is implemented in an integrated circuit.

10. A method according to claim 1, wherein both the primary and secondary entities are implemented in integrated circuits.

11. A method according to claim 1, in which the first entity wishes to communicate with one of the second entities, the method including the steps, in the first entity, of:

receiving data from the second entity;

using the data and the first secret information to generate the second secret information associated with the second entity.

12 A method according to claim 11, wherein the data contains an identifier for the second entity

13. A method according to claim 11, in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of:

using the generated second secret information to sign a message, thereby generating a digital signature;

outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret information.

14. A method according to claim 13 in which the generated signature includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to validate the message using the digital signature, the nonce, and its own copy of the second secret information.

15 A method according to claim 11 wherein the data contains a first nonce.

16 A method according to claim 15 in which the first entity wishes to send an authenticated message to the second entity, the method including the steps, in the first entity, of:

using the generated second secret information and the first nonce to sign a message, thereby generating a digital signature;

outputting the message and the digital signature for use by the second entity, which can validate the message by using the digital signature and its own copy of the second secret information.

17. A method according to claim 16 in which the generated signature includes a second nonce from the first entity, and the output from the first entity includes the second nonce, thereby enabling the second entity to validate the message using the digital signature, the first and second nonces, and its own copy of the second secret information.

18. A method according to claim 11, in which the first entity wishes to send an encrypted message to the second entity, the method including the steps, in the first entity, of:

using the generated second secret information to encrypt a message, thereby generating an encrypted message;

outputting the encrypted message for use by the second entity, which can decrypt the message by using its own copy of the second secret information.

19. A method according to claim 18 in which the encrypted message includes a nonce from the first entity, and the output from the first entity includes the nonce, thereby enabling the second entity to decrypt the message using the nonce, and its own copy of the second secret information.

20. A method according to claim 15, in which the first entity wishes to send an encrypted message that incorporates the first nonce to the second entity, the method including the steps, in the first entity, of:

using the generated second secret information to encrypt a message and the first nonce, thereby generating an encrypted message;

outputting the encrypted message for use by the second entity, which can decrypt the encrypted message by using its own copy of the second secret information.

21. A method according to claim 20 in which the encrypted message includes a second nonce from the first entity, and the output from the first entity includes the second nonce.

22. A method according to claim 1, in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of:

using the second secret information to sign a message, thereby to generate a digital signature; and

outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the digital signature.

23. A method according to claim 1, in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of:

using the second secret information and a nonce to sign a message, thereby to generate a digital signature; and

outputting the message, nonce, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the nonce and digital signature.

24. A method according to claim 1, in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of:

receiving a first nonce from the first entity;

using the second secret information and the first nonce to sign a message, thereby to generate a digital signature; and

outputting the message, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the first nonce and digital signature.

25. A method according to claim 1, in which one of the second entities wishes to send an authenticated message to the first entity, the method including the steps, in the second entity, of:

receiving a first nonce from the first entity;

using the second secret information, the first nonce, and a second nonce to sign a message, thereby to generate a digital signature; and

outputting the message, second nonce, digital signature and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby authenticate the message via the first nonce, second nonce and digital signature.

26. A method according to claim 1, in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of:

using the second secret information to encrypt the message, thereby to generate an encrypted message; and

outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message.

27. A method according to claim 1, in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of:

using the second secret information to encrypt the message and a nonce, thereby to generate an encrypted message; and

outputting the nonce, encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message.

28. A method according to claim 1, in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of:

receiving a nonce from the first entity;

using the second secret information to encrypt the message and the nonce, thereby to generate an encrypted message; and

outputting the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message.

29. A method according to claim 1, in which one of the second entities wishes to send an encrypted message to the first entity, the method including the steps, in the second entity, of:

receiving a first nonce from the first entity;

using the second secret information to encrypt the message and the first nonce and a second nonce, thereby to generate an encrypted message; and

outputting the second nonce, the encrypted message and the second entity's identifier for use by the first entity, such that the first entity can use the identifier and the first secret information to generate the second secret information associated with the second entity, and thereby decrypt the encrypted message.

30. A method according to any one of claims 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 27, 28 or 29, wherein at least one of the nonces is a pseudo-random number.

31. A method according to any one of claims 11 to 21, wherein the communication is an authenticated read of a field of the first entity.

32. A method according to any one of claims 22 to 29, wherein the communication is an authenticated read of a field of the second entity.